



# APPUNTI S&R (PIETRO VACCARI)

(Il livello delle applicazioni nei modelli ISO/OSI e TCP/IP) e (I protocolli a livello di applicazione: HTTP, FTP, SMTP, POP, IMAP, DNS)

ISO/OSI

Livello 7 (ISO/OSI) - Il Livello Applicazione

TCP/IP

Livello 4 (TCP/IP) - Il Livello Applicazione

La sicurezza nei sistemi informativi, tipologie di attacchi informatici

Tipi di minacce

Obbiettivi della sicurezza

3 Pilastri della sicurezza

Processo di stima dei rischi

Tipi di attacco

La sicurezza delle connessioni con SSL/TLS; HTTPS

EVOLUZIONE:

Funzionamento del TLS:

VPN

Firewall, Proxy, ACL e DMZ

FIREWALL

ACL Access Control List

Classificazione dei firewall

Personal firewall

Network firewall

Packet filter router

PROXY

DMZ

Business continuity e disaster recovery

Wireless: comunicare senza fili

Trasmissione wireless

WLAN

Accesso alla WLAN

Tipi di onde: Infrarossi e Radio

Il protocollo 802.11

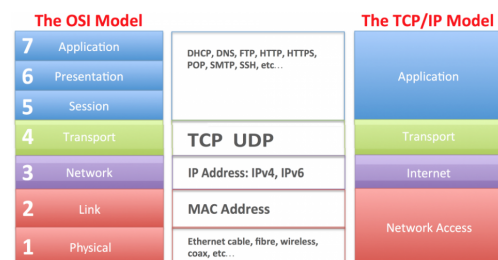
Tipologie di Reti Mobili

[Autenticazione nelle reti wireless](#)  
[Le applicazioni e i sistemi distribuiti](#)  
[Architetture dei sistemi web](#)  
[API](#)  
[Socket](#)  
[La comunicazione seriale](#)  
[Posta elettronica](#)  
[Porte delle applicazioni](#)  
[Sintassi di una richiesta HTTP](#)  
[Multiplexing](#)

## (Il livello delle applicazioni nei modelli ISO/OSI e TCP/IP) e (I protocolli a livello di applicazione: HTTP, FTP, SMTP, POP, IMAP, DNS)

### ISO/OSI

(Open Systems Interconnection): Il modello OSI contiene sette livelli disposti concettualmente dal basso verso l'alto. I livelli ISO OSI sono: Fisico, Collegamento Dati, Rete, Trasporto, Sessione, Presentazione, e Applicazione.



### Livello 7 (ISO/OSI) - Il Livello Applicazione

Il livello 7 è quello con cui la maggior parte delle persone ha familiarità perché comunica direttamente con l'utente. Un'applicazione che gira su un dispositivo può comunicare con altri livelli OSI, ma l'interfaccia viene eseguita sul livello 7. Quando un messaggio viene ricevuto dal client, il livello applicazione è ciò che lo presenta agli occhi dell'utente. I protocolli di applicazione includono l'SMTP (Simple Mail Transfer Protocol) e l'HTTP, che costituisce il protocollo per la comunicazione tra browser e web server.

### TCP/IP

- IP (Internet Protocol);
- TCP (Transmission Control Protocol).

L'architettura del modello TCP/IP si basa solo su quattro livelli, a differenza del modello ISO/OSI che ne prevede sette.

- Il protocollo UDP (User Datagram Protocol) è un protocollo di trasporto non affidabile, non orientato alla connessione, che non garantisce l'arrivo dei dati a destinazione in modo corretto e in ordine. La comunicazione con il protocollo UDP non prevede una fase di handshake per stabilire i parametri di trasmissione e i dati vengono trasmessi senza garantire la corretta ricezione. Questo protocollo viene utilizzato quando la perdita di alcuni dati non è critica o quando è necessario un tempo di latenza minimo.
- Il protocollo TCP (Transmission Control Protocol) è un protocollo di trasporto affidabile, orientato alla connessione, che garantisce l'arrivo dei dati a destinazione in modo corretto e in ordine. La comunicazione con il protocollo TCP richiede l'apertura di una connessione tra il mittente e il destinatario, che prevede una fase di handshake per stabilire i parametri di trasmissione. Una volta stabilita la connessione, i dati vengono trasmessi attraverso il canale di comunicazione. Il protocollo TCP garantisce la corretta ricezione dei dati tramite il controllo di flusso, il controllo degli errori e la ritrasmissione dei pacchetti persi.
- Il protocollo IP fornisce l'instradamento dei pacchetti in modalità detta best-effort delivery ("miglior sforzo per spedire a destinazione"). Questa non è affidabile e non effettua la correzione di errore. Inoltre non effettua alcun controllo sulla congestione e sul flusso.

Quando un'applicazione invia dei dati utilizzando l'architettura TCP/IP, questi seguono un percorso "dall'alto verso il basso" attraverso tutti i livelli della pila fino a essere trasmessi dal livello fisico. Ogni livello aggiunge una serie di informazioni di controllo ai primi dati che riceve, gli header (intestazione), fino a giungere al livello di rete che, oltre all'intestazione aggiunge anche alcuni dati in coda (il cosiddetto trailer).

- Lo strato di applicazione aggiunge un'intestazione (header-app) ai dati utente prima di passarli allo strato di trasporto.
- Il protocollo TCP (oppure UDP) dello strato di trasporto aggiunge anch'esso un'intestazione: l'unità di dati prende ora il nome di segmento e viene passata allo strato di rete.

- Lo **strato di rete** acclude a sua volta un'intestazione comprendente l'indirizzo IP: a questo punto il dato assume la denominazione di datagramma IP.

Questa unità di informazione viene infine passata ai livelli inferiori, dove lo strato di collegamento aggiunge la propria intestazione (header) e una coda (trailer): siamo finalmente arrivati alla trama (frame ethernet)

## Livello 4 (TCP/IP) - Il Livello Applicazione

Il livello di applicazione (o Application Layer) comprende tutti i protocolli di alto livello e di dialogo con l'utente, tra cui quelli specifici per il trasferimento di file, le e-mail, il login remoto.

- Alcuni dei protocolli presenti a questo livello sono:
- **HTTP** (Hypertext Transfer Protocol): è un protocollo di comunicazione utilizzato per la trasmissione di informazioni sulla rete. Funziona tramite richieste e risposte tra client e server. Il client invia una richiesta utilizzando un metodo (ad esempio GET o POST) e specificando un'URL per indicare la risorsa richiesta. Il server risponde con un codice di stato (ad esempio 200 OK) e i dati richiesti.
- **FTP** (File Transfer Protocol): è un protocollo utilizzato per la trasmissione di file tra computer sulla rete. FTP consente agli utenti di accedere ai file su un server remoto e di trasferirli sulla loro macchina locale.
- **SMTP** (Simple Mail Transfer Protocol): è un protocollo utilizzato per la trasmissione di email su Internet. SMTP viene utilizzato per inviare email dal client email del mittente al server email del destinatario.
- **POP** (Post Office Protocol): è un protocollo utilizzato per la ricezione di email su un client email. POP consente al client email di scaricare le email dal server email del provider.
- **IMAP** (Internet Message Access Protocol): è un protocollo utilizzato per la ricezione di email su un client email. IMAP consente al client email di accedere alle email sul server email del provider e di visualizzarle senza doverle scaricare.
- **DNS** (Domain Name System): è un protocollo utilizzato per la risoluzione dei nomi di dominio in indirizzi IP. DNS consente agli utenti di accedere ai siti web utilizzando un nome di dominio comprensibile anziché l'indirizzo IP numerico.

## La sicurezza nei sistemi informativi, tipologie di attacchi informatici

La sicurezza nei sistemi informativi è una disciplina che si occupa di proteggere le informazioni e i dati all'interno di un sistema informatico dalle minacce esterne. Le tipologie di attacchi informatici sono molteplici e in costante evoluzione.

## Tipi di minacce

- **NATURALI**: è l'insieme delle minacce che non dipendono da attacchi / errori umani (inondazioni, terremoti, blackout).
- **UMANE**: è l'insieme delle minacce che dipendono da uno o più esseri umani (attacchi, sicurezza mal gestita).

## Obiettivi della sicurezza

- Garantire il **PRINCIPIO MINIMO DI SICUREZZA**: 1) essere protetto dagli attacchi passivi, 2) eseguire analisi periodiche per prevenire attacchi attivi.
- **Autenticazione**: processo mediante il quale un sistema verifica l'identità di un utente o di un dispositivo.
- **Autorizzazione**: processo di concessione o negazione di accesso a risorse informatiche specifiche da parte di utenti o dispositivi autenticati.
- **Riservatezza**: garanzia che le informazioni siano accessibili solo a coloro che hanno il permesso di accedervi.
- **Disponibilità**: garanzia che le informazioni e le risorse siano disponibili e accessibili agli utenti autorizzati quando necessario.
- **Integrità**: garanzia che le informazioni siano complete, accurate e non manipolate.
- **Paternità**: garanzia che le informazioni siano attribuite correttamente all'autore o all'origine appropriata.

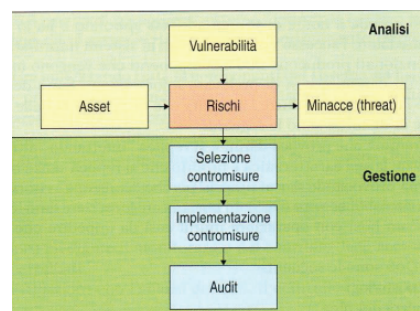
## 3 Pilastri della sicurezza

- **Prevenzione** (avoidance) mediante protezione dei sistemi e delle comunicazioni (crittografia, firewall, VPN).
- **Rilevazione** (detection) mediante il monitoraggio e il controllo degli accessi tramite autenticazione con password e certificati.
- **Investigazione** (investigation) con l'analisi dei dati, il controllo interno con il confronto e la collaborazione degli utenti ecc.

## Processo di stima dei rischi

Il processo di stima dei rischi in una rete informatica è un'attività fondamentale per garantire la sicurezza e la protezione delle informazioni e delle risorse. Il processo può essere suddiviso in diversi passaggi:

1. Identificazione delle informazioni e delle risorse critiche: in questa fase si individuano le informazioni e le risorse di maggior valore o importanza all'interno della rete informatica. Ciò può includere dati sensibili, informazioni personali, informazioni di proprietà dell'azienda o risorse hardware o software di fondamentale importanza per il corretto funzionamento del sistema.
2. Identificazione delle minacce: in questa fase si individuano tutte le possibili minacce alla sicurezza delle informazioni e delle risorse, come ad esempio attacchi informatici, accessi non autorizzati, errori umani, malfunzionamenti hardware o software, calamità naturali, ecc.
3. Analisi dei rischi: in questa fase si valutano le probabilità di accadimento di ogni minaccia e il relativo impatto sui sistemi informatici. L'analisi viene effettuata in modo quantitativo o qualitativo, attraverso strumenti specifici.
4. Valutazione dei controlli di sicurezza: in questa fase si analizzano i controlli di sicurezza esistenti all'interno della rete informatica e si valutano la loro efficacia nel mitigare i rischi individuati.
5. Identificazione di misure di mitigazione dei rischi: in questa fase si individuano le misure di mitigazione necessarie per ridurre i rischi individuati. Ciò può includere l'implementazione di nuovi controlli di sicurezza, l'aggiornamento di software, la formazione degli utenti, ecc.
6. Monitoraggio e revisione: il processo di stima dei rischi in una rete informatica è un processo continuo, che richiede un costante monitoraggio e revisione delle informazioni e dei rischi. Ciò consente di individuare e gestire eventuali nuove



(ASSET: insieme dei dati e persone necessarie all'erogazione del servizio).

(AUDIT: valutazione finale).

minacce o rischi e di adattare costantemente i controlli di sicurezza per garantire la massima protezione possibile.

## Tipi di attacco

- **PASSIVI:**
  - Lettura del contenuto ad esempio mediante lo sniffing di pacchetti sulla LAN;
  - Analisi del sistema e del traffico di rete, senza analizzare i contenuti.
- **ATTIVI:**
  - **Intercettazione:** a differenza di quella passiva che si limita a “spiare” i dati (packet sniffing), quella attiva mira a intercettare le password per avere accesso al sistema ed effettuare modifiche ai dati. È possibile che per effettuare l'intercettazione sia necessario un attacco preventivo per installare componenti hardware (dispositivi pirata) o software specifici. Ad esempio, potrebbero essere inseriti nella rete dei server pirata (shadow server) che si spacciano per i server originali nei quali sono state modificate le tabelle di routing (spoofing) oppure possono essere installati programmi che emulano servizi del sistema registrando al contempo le informazioni riservate digitate dall'utente: potrebbe essere sostituito il programma di login così che quando un utente si connette gli viene intercettata la password (password cracking).
  - **Sostituzione di un host:** sempre tramite la modifica delle tabelle di indirizzamento dei router (IP spoofing) qualcuno si sostituisce a un host falsificando l'indirizzo di rete del mittente (solitamente si falsifica l'indirizzo di livello 3 (IP) ma nulla vieta di falsificare anche quello di livello 2). Questo tipo di attacco prende il nome di source address spoofing e ha lo scopo di effettuare la falsificazione di dati mediante l'accesso non autorizzato ai sistemi informativi.
  - **Produzione:** i malintenzionati producono nuovi componenti che vengono inseriti nel sistema con lo scopo di produrre un danno, e non di prelevare informazioni. Sono dei veri e propri atti di sabotaggio che hanno l'obiettivo di ridurre l'integrità e la disponibilità delle risorse del sistema. Le principali tecniche di disturbo sono le seguenti:
    - **attacchi virus:** programma che provoca danni e si replica “infettando” altri host.

- attacchi tramite **worm**: la sua caratteristica è proprio che si replica senza bisogno di “attaccarsi” a un altro programma provocando danni proprio perché “consuma” risorse.
- attacchi di disturbo denial of service (**DoS**): in questa categoria rientrano le tecniche che mirano a “tenere occupato” un host con operazioni inutili così da impedire che possa offrire i propri servizi alla rete. Alcune tecniche di DoS sono le seguenti:
  - saturazione della posta/log.
  - ping flooding (“guerra dei ping”).
  - SYN attack.
  - distributed denial-of-service (**DDoS**): viene installato un software per DoS su molti nodi costituendo una Botnet: questi programmi sono anche chiamati daemon, zombie o malbot (i daemon sono generalmente controllati remotamente da un master tramite canali cifrati e hanno capacità di auto-aggiornamento).
- **Phishing**: attraverso spamming di email si attrae un utente su un server pirata (shadow server): in modo da catturare le credenziali di autenticazione o altre informazioni personali; oppure viene invitato l'utente a installare un plugin o una estensione che in realtà sono o virus o trojan. Una variante evoluta è lo spear phishing che include nella mail molti dati personali per aumentare la credibilità del messaggio.
- **Intrusione**: l'intrusione è l'accesso vero e proprio non autorizzato a uno o più host, che può essere il risultato delle tecniche prima descritte: una volta che un intruso si è introdotto in un sistema può modificare o cancellare le informazioni altrui, prelevare i dati che gli interessano, introdurre dati falsi ecc.

## La sicurezza delle connessioni con SSL/TLS; HTTPS

**SSL/TLS** è un protocollo crittografico utilizzato per garantire la sicurezza delle comunicazioni tra client e server su Internet. **SSL (Secure Sockets Layer)** è stato il primo protocollo di sicurezza a essere utilizzato, ma è stato sostituito da **TLS (Transport Layer Security)** che è più sicuro.



SSL/TLS utilizza un sistema di crittografia a chiave pubblica per garantire che i dati scambiati tra il client e il server siano protetti da terze parti. In particolare, il client e il server stabiliscono una connessione crittografata utilizzando un certificato digitale rilasciato da un'autorità di certificazione.

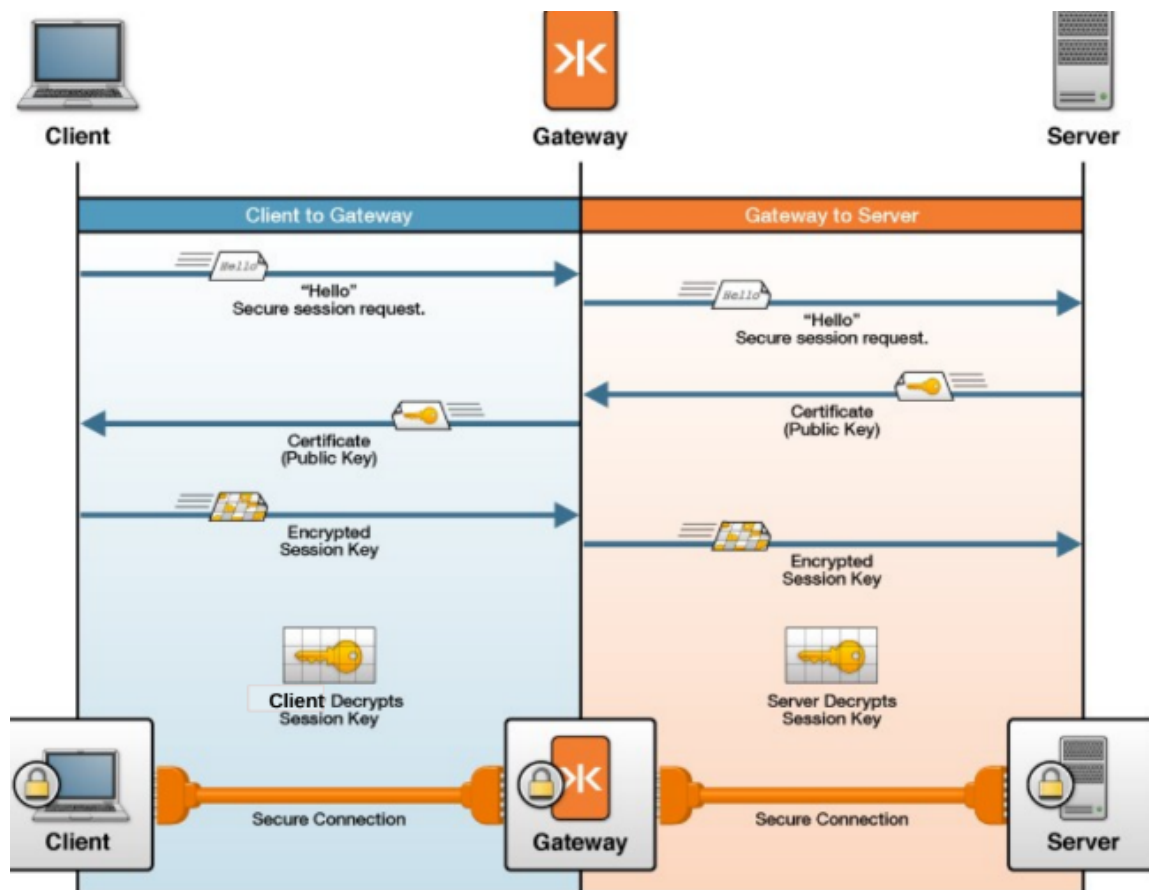
Secure Socket Layer (SSL) ⇒ sicurezza a livello SESSIONE (OSI) con funzionalità di cifratura ed autenticazione DES ed RSA

## EVOLUZIONE:

1. Nasce come SSL con il browser Netscape Navigator (antesignano di Mozilla-Firefox).
2. Si evolve con SSL/TLS, protocollo standardizzato come Transport Layer Security fra client e server certificati.
  - **HTTPS: Combinazione di http con SSL-TLS** (porta 443).
  - **S-HTTP**: Incapsulamento messaggi crittografati in formato MIME/CMS.
  - **SMTPS** :465 **POPS** :995 **IMAPS** :993 Combinazione con gli standard di invio/ricezione messaggi di posta elettronica.

## Funzionamento del TLS:

- **TLS record protocol**: Opera appena sopra il livello trasporto affidabile (TCP), suddividendo in blocchi i dati del livello superiore, calcolando il MAC e cifrando.
- **TLS handshake protocol**: Opera nella fase di negoziazione della connessione e si divide in:
  - **Handshake protocol**: Instaurazione connessione.
  - **Change cipher spec**: Scambio chiavi e certificati fra client e server.
  - **Alert protocol**: Segnala problemi nella sessione SSL.



La fase di definizione della session key si divide prevede **premaster key** generata dal client grazie al certificato che contiene la chiave pubblica e quindi la **decifrazione della chiave di sessione** da parte del server con la sua chiave privata.

**HTTPS** (HyperText Transfer Protocol Secure) è una versione sicura del protocollo HTTP utilizzata per le comunicazioni web. HTTPS utilizza SSL/TLS per crittografare le comunicazioni tra il browser del client e il server web, garantendo la privacy e l'integrità dei dati scambiati. La connessione HTTPS viene identificata dall'URL "https" e dalla presenza di un lucchetto nella barra degli indirizzi del browser.

## VPN

Una VPN (Virtual Private Network) è una tecnologia di rete che consente di creare una connessione sicura e crittografata tra un dispositivo e una rete privata su Internet.

In pratica permette di connettersi a Internet attraverso un server remoto che funge da "ponte" tra il dispositivo dell'utente e la rete privata. In questo modo, tutti i dati

trasmessi tra il dispositivo e la rete privata vengono criptati, rendendoli inaccessibili a terze parti.

Le VPN vengono utilizzate principalmente per proteggere la privacy degli utenti su Internet. Ad esempio, una persona che utilizza una VPN può nascondere il proprio indirizzo IP e la propria posizione geografica, impedendo ai siti web e agli hacker di tracciare le proprie attività online.

A livello tecnico utilizzano diversi protocolli per creare una connessione sicura tra il dispositivo dell'utente e la rete privata a cui si vuole accedere.

Il protocollo più comunemente utilizzato per creare una VPN è il protocollo OpenVPN, che utilizza la crittografia SSL/TLS per creare una connessione sicura tra il dispositivo e il server.

Per creare la connessione, il client VPN (cioè il software installato sul dispositivo dell'utente) e il server VPN devono scambiarsi informazioni di autenticazione, come le credenziali di accesso dell'utente e le chiavi di crittografia. Queste informazioni sono protette da un processo di autenticazione forte, che prevede l'uso di password complesse e/o di un token di autenticazione generato da un'applicazione dedicata.

Una volta che la connessione VPN è stata stabilita, tutti i dati trasmessi tra il dispositivo e il server VPN vengono criptati utilizzando algoritmi di crittografia sicuri come AES (Advanced Encryption Standard).

Il client può anche essere configurato per utilizzare diversi protocolli VPN, tra cui PPTP, L2TP/IPsec e IKEv2. Ogni protocollo presenta vantaggi e svantaggi in termini di sicurezza, velocità e compatibilità con i diversi dispositivi.

## Firewall, Proxy, ACL e DMZ

### FIREWALL

E' un meccanismo che consenta di controllare "il traffico in transito" e, tramite regole appositamente configurate, di inibire e/o permettere l'accesso agli indesiderati.

Nel caso di un attacco a una LAN la zona più esposta è quella intermedia e l'attaccante deve superare le difese successive del firewall che regola e limita il traffico tra i server front-end e back-end che comunicano tra loro solo su porte TCP o UDP strettamente necessarie e ben controllate.

Un firewall è un **sistema hardware-software** dedicato alla difesa perimetrale di una rete che agisce filtrando il traffico di pacchetti entranti e/o uscenti secondo delle

regole precedentemente definite. Generalmente un firewall di rete è costituito da più macchine differenti che lavorano assieme per prevenire accessi non voluti: il **router esterno**, quello connesso a Internet, invia tutto il traffico entrante all'**application gateway** che seleziona i pacchetti utilizzando apposite **liste di accesso** (ACL Access control list) e li inoltra alla **rete interna**: quindi il gateway filtra il traffico entrante e uscente, eliminando i pacchetti che non soddisfano i requisiti di sicurezza individuati (**filtering router**).

Nella **progettazione di un firewall** bisogna tenere presente tre principi fondamentali.

1. Il firewall deve essere l'unico punto di contatto della rete interna con quella esterna.
2. Solo il traffico "autorizzato" può attraversare il firewall.
3. Il firewall deve essere un sistema altamente sicuro esso stesso.

## ACL Access Control List

Le regole vengono disposte in liste apposite chiamate **ACL (Access Control List)** dove è possibile dettagliare i filtri da applicare a ogni pacchetto in funzione delle informazioni presenti negli header TCP/IP, quindi a livello 3 (networking); a volte vengono analizzati anche gli header di livello 4 (transport) ma si ignorano le informazioni del protocollo applicativo al quale il pacchetto si riferisce.

Le ACL si basano o su indirizzo sorgente o destinazione o sui protocolli e sui numeri di porta dei livelli superiori e le filosofie alla loro base sono due, tra loro opposte:

- **open security policy**: tutto è permesso per default e nella lista ACL è presente l'elenco dei divieti.
- **closed security policy**: tutto è vietato per default e nella lista ACL sono elencati i pochi accessi che vengono permessi, ed è la politica maggiormente adottata.

Le ACL possono anche essere inserite su qualunque router anche se trovano la loro applicazione ottimale nei router firewall posizionati tra i router interni e Internet.

## Classificazione dei firewall

Una prima differenziazione viene fatta sul tipo di protezione che il firewall deve fare: come già detto, è possibile avere attacchi sia dall'esterno che dall'interno, quindi la prima classificazione riguarda proprio:

- **ingress firewall** : vengono controllati i collegamenti incoming, gli accessi ai servizi che sono offerti all'esterno della LAN;
- **egress firewall**: vengono controllati collegamenti outgoing, cioè l'attività del personale interno nella LAN verso l'esterno, in modo da filtrare il traffico in modo che quello non autorizzato o doloso non lasci mai la rete interna.

Il secondo tipo di classificazione prevede il numero di host protetti contemporaneamente:

- **personal firewall**: proteggono il singolo host consentendo, generalmente di default, qualsiasi traffico verso l'esterno (outbound) e bloccando quello dall'esterno (inbound);
- **network firewall**: si interpone fra la LAN e Internet e controlla tutto il traffico passante.

Un terzo tipo di classificazione viene fatta a seconda del livello di intervento:

- **filtri di pacchetto IP**: permettono di bloccare o abilitare selettivamente il traffico che attraversa il firewall, definendo i protocolli (o meglio, il tipo di pacchetto), gli indirizzi IP e le porte utilizzate;
- **server proxy**: rappresentano una sorta di intermediario che si occupa di intrattenere le connessioni per conto di qualcun altro nella rete interna.

## Personal firewall

Un personal firewall può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni: in essi il traffico dall'interno verso l'esterno è consentito per default mentre il traffico dall'esterno verso l'interno è vietato per default.

I personal firewall sono utilizzabili solo a scopo personale ma impensabili in una azienda in quanto risulterebbero economicamente non convenienti e inoltre sarebbe difficile implementare una politica comune delle policy, dovendo configurare ogni singolo host manualmente.

## Network firewall

Sono i classici firewall aziendali dove una (o più) macchine sono dedicate al filtraggio di tutto il traffico da e per una rete locale e solo il traffico autorizzato deve attraversare il firewall facendo in modo di mantenere i servizi di rete ritenuti necessari.

A seconda del **livello di rete** nel quale si fanno i controlli i network firewall possono essere classificati in:

- **packet-filtering router**: network level gateway.
- **circuit gateway**: gateway a livello di trasporto.
- **proxy server**: gateway a livello di applicazione.

## Packet filter router

Un packet filtering router **scherma i pacchetti** dipendentemente dal tipo di protocollo, dall'indirizzo della sorgente e della destinazione e dai campi di controllo presenti nei pacchetti in transito, cioè **analizza le informazioni contenute nell'header TCP/IP** a livello di rete e di trasporto (packet inspection) per individuare:

- **IP del mittente o del destinatario**.
- **indirizzo MAC sorgente o di destinazione**.
- **numero di porta verso cui è destinato il pacchetto**.
- **protocollo da utilizzare**.

Il firewall decide se il pacchetto può essere accettato o meno attraverso un **algoritmo di scelta** che si basa su una **lista di regole** (in ordine di priorità) precedentemente definite: le filosofie applicabili come regola di funzionamento sono quindi due, diametralmente opposte:

- ciò che **NON è specificatamente permesso è proibito (deny)**.
- ciò che **NON è specificatamente proibito è permesso (permit)**.

e le regole di controllo possono essere configurate in modo statico (manuale) con validità temporale illimitata, oppure dinamico.

Quindi in base a queste regole i pacchetti possono essere:

- **accept/allow**: il firewall **permette al pacchetto di raggiungere la sua destinazione**.
- **deny**: il firewall **scarta il pacchetto**, senza che questo passi attraverso il firewall e viene inviato un **messaggio d'errore all'host sorgente**.
- **discard/reject**: il firewall **scarta il pacchetto senza restituire nessun messaggio d'errore all'host sorgente**, implementando quella che viene chiamata **metodologia black hole**, che **elimina il pacchetto senza che la sua presenza venga rivelata agli estranei**.

## PROXY

Un gateway a livello di applicazione permette di realizzare una politica di sicurezza molto più severa di un semplice packet filtering router: in esso non vengono analizzati e filtrati i pacchetti ma vengono gestite le applicazioni utilizzando un apposito programma detto **proxy**.

Il proxy è un programma che viene eseguito sul gateway che funge da intermediario a livello di applicazione, ad esempio tra il computer dell'utente e Internet; nelle applicazioni client-server un application proxy comunica con il client simulando di essere il server, e viceversa, comunica con il server simulando di essere il client.

Mentre un packet filter è capace di utilizzare soltanto informazioni di basso livello come indirizzi IP e numero di porta, un application proxy è in grado di ispezionare l'intera porzione dati del pacchetto ed è in grado di bloccare pacchetti FTP che contengono certi nomi di file, così da inibire la connessione con determinate pagine o siti Web.

I principali **vantaggi** nell'utilizzo di un gateway a livello di applicazione sono:

- **controllo completo**: dato che utilizza anche le informazioni contenute nel body, effettua un doppio controllo, sia quando viene inviata la richiesta che quando si riceve la risposta.
- **log dettagliati**: avendo a disposizione anche le informazioni di livello applicativo produce dei file di log molto accurati.
- **nessuna connessione diretta**: tutti i dati in transito sono analizzati e ricostruiti: tentativi di buffer overflow o simili sono intercettati e non vengono inoltrati all'host interno.
- **sicurezza anche in caso di crash**: nel caso di un crash del proxy la LAN risulta isolata e quindi inaccessibile dall'esterno rimanendo protetta.
- **supporto per connessioni multiple**: è in grado di gestire connessioni separate che appartengono alla stessa applicazione.
- **user-friendly**: è semplice configurare le regole di filtraggio rispetto a quelle di un packet filtering router.
- **autenticazione e filtraggio dei contenuti**: offre anche il servizio autenticazione dell'utente e il riconoscimento dei contenuti.
- **cache**: effettua il caching delle pagine Web e quindi offre un ulteriore servizio liberando la rete da traffico inutile nel caso di richiesta della stessa pagina.

Per contro, gli **svantaggi** nell'uso di un gateway a livello di applicazione sono:

- è poco trasparente: richiede che ogni computer della LAN interna sia configurato per utilizzare il proxy.
- richiede un proxy per ogni applicazione: è necessario dedicare un proxy a ogni servizio che si ha necessità di far passare attraverso il firewall e, data la dinamicità con la quale vengono offerti servizi in rete, è necessario il suo continuo aggiornamento.
- ha basse performance: la gestione della connessione attraverso il proxy richiede molto lavoro per la CPU e quindi ha prestazioni molto inferiori rispetto ai firewall delle generazioni recedenti.

## DMZ

DMZ è la sigla di **Demilitarized Zone (zona demilitarizzata)** ed è una “sezione di rete” delicata e importante per i processi di sicurezza.

La zona demilitarizzata è una porzione di rete che separa la rete interna dalla rete esterna: i server nella DMZ sono accessibili dalla rete pubblica, perciò non sono trusted (dalla rete interna) e quindi devono essere segregati in quanto, se venissero compromessi, questo non deve produrre effetti collaterali nella rete aziendale.

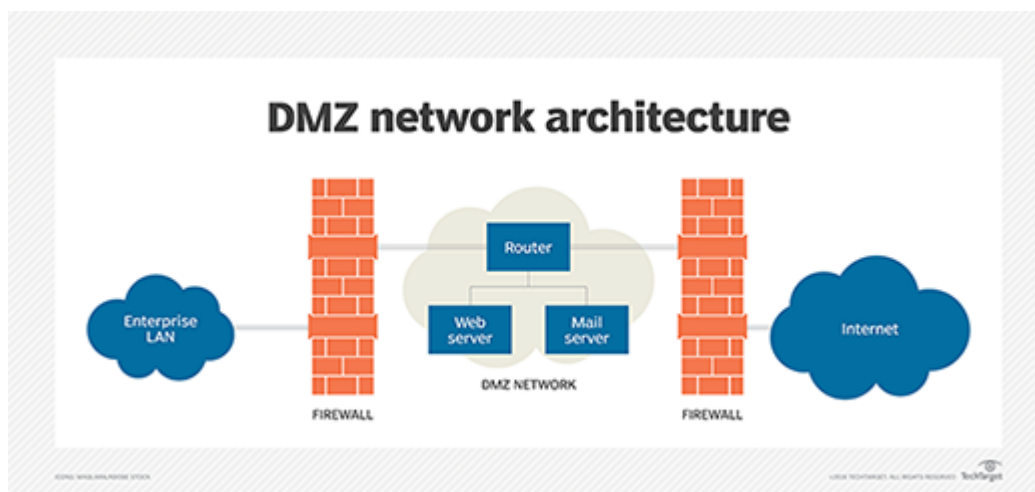
La DMZ permette di effettuare la sicurezza perimetrale, cioè protegge una rete nei punti in cui essa è a contatto con il mondo esterno, interponendosi tra la LAN aziendale e la WAN esterna:

- il lato LAN (local area network) è il segmento privato e protetto, e a esso appartengono tutti gli host e i server i cui servizi sono riservati all'uso interno.
- la zona WAN (wide area network) è la parte esterna, e a essa appartengono uno o più apparati di routing che sostengono il traffico da e per la rete locale, sia verso Internet che verso eventuali sedi remote dell'azienda.

La principale difesa contro gli attacchi a una rete è proprio una corretta organizzazione topologica della rete stessa; l'approccio ormai condiviso è quello di suddividere la rete in zone di sicurezza in modo che:

- i dispositivi e le risorse sono posizionati nelle zone in base ai loro livelli e requisiti di sicurezza.
- la rete acquisisce una maggiore scalabilità e una conseguente maggiore stabilità.





## Business continuity e disaster recovery

- **BUSINESS CONTINUITY**: capacità di un'organizzazione di mantenere le sue attività operative in caso di interruzione o fallimento di uno o più dei suoi processi critici. In altre parole, è la capacità di un'organizzazione di continuare a funzionare nonostante gli eventi avversi. La business continuity si concentra sulle soluzioni per ridurre al minimo gli impatti negativi di situazioni di emergenza.
- **DISASTER RECOVERY**: è l'insieme delle misure che un'organizzazione adotta per recuperare le sue attività in seguito a una situazione di emergenza o di disastro. Questo può includere il ripristino dei sistemi IT, la ricostruzione dei dati, la creazione di nuove infrastrutture o la sostituzione di attrezzature danneggiate. L'obiettivo del disaster recovery è di minimizzare il tempo di inattività e di riprendere le attività il più rapidamente possibile.

Per implementare business continuity e disaster recovery, le organizzazioni adottano solitamente una serie di procedure e di soluzioni tecnologiche, tra cui:

- Backup dei dati: l'organizzazione deve eseguire regolarmente il backup dei dati in modo da poterli ripristinare in caso di perdita o di distruzione.
- Replicazione dei dati: l'organizzazione può utilizzare la replica dei dati per mantenere una copia esatta dei dati in un luogo diverso dal sito primario.
- Archiviazione di backup offline: i backup critici possono essere archiviati in un luogo sicuro offline per prevenire la loro compromissione in caso di attacchi informatici.

- Piani di emergenza: l'organizzazione deve sviluppare e testare piani di emergenza per ogni possibile scenario di interruzione delle attività.
- Soluzioni di continuità: l'organizzazione può utilizzare soluzioni di continuità del business come la replica dell'intera infrastruttura IT in un sito alternativo.
- Soluzioni di disaster recovery: l'organizzazione può utilizzare soluzioni di disaster recovery come la replicazione delle applicazioni e dei dati in un sito alternativo.

## Wireless: comunicare senza fili

Il wireless è una tecnologia che consente la comunicazione senza fili tra dispositivi e sistemi di rete, consentendo la connessione tra dispositivi senza la necessità di un cavo fisico. La connessione wireless è utilizzata per creare reti locali wireless (WLAN) o per connettersi a reti esterne tramite tecnologie come il Wi-Fi.

Per creare una WLAN, è necessario un access point wireless (WAP) che agisca come hub per la connessione tra i dispositivi. Il WAP riceve e trasmette i dati attraverso l'etere, il mezzo di trasmissione wireless, e gli altri dispositivi si connettono all'access point per accedere alla rete.

Ci sono diverse tecnologie wireless utilizzate per la comunicazione nel campo dell'informatica. Il Wi-Fi, ad esempio, è una tecnologia basata sullo standard IEEE 802.11 e utilizza frequenze radio per trasmettere dati tra dispositivi. Il Bluetooth è un'altra tecnologia wireless utilizzata per la connessione tra dispositivi a breve distanza.

## Trasmissione wireless

La trasmissione wireless è la tecnologia che consente di trasferire dati tra dispositivi senza l'utilizzo di un cavo fisico. La trasmissione wireless avviene attraverso l'invio di onde elettromagnetiche, che si propagano nell'aria o nello spazio libero.

Per la trasmissione il segnale elettrico che contiene i dati viene convertito in una forma di energia elettromagnetica, che può essere trasmessa attraverso l'antenna del dispositivo. Il segnale trasmesso viene poi ricevuto dall'antenna del dispositivo di destinazione, che lo converte nuovamente in un segnale elettrico.

Le tecnologie più comuni sono Wi-Fi, Bluetooth, NFC e cellulari. Ogni tecnologia utilizza un tipo specifico di onda elettromagnetica, che può essere modulata per trasportare informazioni in diverse frequenze.

La trasmissione wireless presenta diversi vantaggi, come la flessibilità nell'installazione e nell'uso dei dispositivi, la mobilità e la possibilità di connettere dispositivi remoti. Tuttavia presenta anche alcune limitazioni, come la sensibilità alle interferenze e alle distanze, la necessità di dispositivi compatibili e la sicurezza delle comunicazioni. Per garantire la sicurezza delle trasmissioni vengono utilizzati protocolli di crittografia e autenticazione, come WPA e WPA2 per le reti Wi-Fi, che assicurano la privacy delle informazioni trasmesse e proteggono la rete da eventuali attacchi informatici.

## WLAN

La LAN con accesso wireless prende anche il nome di WLAN. Quando un dispositivo vuole connettersi a una WLAN esegue uno scanning alla ricerca di un AP (AccessPoint) compatibile con il quale eseguire l'associazione.

Lo scanning può essere:

- Attivo (active): il client lancia una richiesta per unirsi alla LAN contenente un SSID (Service Set Identifier) e, se viene accettata analizzando le credenziali del richiedente e controllando gli eventuali diritti di accesso, l'AP gli risponde permettendogli il collegamento.
- Passivo (passive): il client si pone in ascolto di messaggi (bacon) trasmessi dall'AP in attesa di riceverne uno contenente l'SSID della rete alla quale desidera connettersi.

## Accesso alla WLAN

L'SSID è il nome con cui una rete Wi-Fi si presenta ai suoi utenti: consiste in genere in una serie di caratteri ASCII stampabili e viene continuamente trasmesso in modo che gli utenti possano individuare la presenza della rete di loro interesse alla quale connettersi.

L'autenticazione per l'accesso a una WLAN è a livello 2 e quindi viene autenticato il dispositivo e non l'utente: se la LAN offre un servizio di "sistema aperto", cioè permette libero accesso ad alcuni servizi (tipo la connessione Internet) da parte di chiunque ne faccia esplicita richiesta (è sufficiente che coincidano il SSID della LAN e del client).

Per accessi a rete privata o LAN aziendali l'AP viene configurato per inviare la richiesta a un server di autenticazione oppure può effettuare direttamente la validazione mediante una chiave condivisa: in questo caso è richiesta la crittografia

WEP (Wireless Equivalent Protocol) a 64 o 128 bit della comunicazione per evitare intrusioni indesiderate: all'AP e a tutti i nodi viene assegnata staticamente la chiave di accesso, e dal semplice confronto di questa si determina l'autenticazione del client. A seguito dell'autenticazione l'AP effettua l'associazione e quindi autorizza il client a connettersi alla rete e a trasferire i dati.

## Tipi di onde: Infrarossi e Radio

- La tecnologia a raggi infrarossi può essere utilizzata solo in uno spazio aperto o all'interno di un singolo locale essendo estremamente sensibile agli ostacoli.
- Per una rete locale che si estende all'interno di edifici l'unica soluzione è quella che utilizza le onde radio: il protocollo 802.11 prevede infatti che la propagazione dei segnali avvenga utilizzando questo tipo di onde.
- Le trasmissioni occupano una banda di frequenze che viene suddivisa in tanti canali tra loro separati.
- Per trasmettere su un particolare canale è necessario possedere il rispettivo codice di autorizzazione.

## Il protocollo 802.11

- Per reti non cablate: pensato per gestire il colloquio fra tante stazioni che comunicano tra loro in modo paritetico.
- Per reti cablate: pensato per l'accesso a una rete più articolata da parte di un dispositivo per la realizzazione di Distributed System (Sistema di distribuzione dell'informazione).
- 802.11: i dispositivi comunicano tra loro a 2.4 GHz con velocità da 1 a 2 Mbps.
- 802.11b: arriva fino a 11 Mbps ed è chiamata Wi-Fi o wireless ad alta velocità.
- 802.11a: per i dispositivi wireless che operano a 5 GHz e arrivano fino a 54 Mbps.
- 802.11g: utilizza tecniche di modulazione OFDM(Orthogonal Frequency-Division Multiplexing).
- Nel protocollo sono definite:
  - le modalità in cui diverse stazioni costituiscono un'Ad Hoc Network, cioè una rete ad hoc wireless in ambito locale.

- le modalità per cui le stazioni appartenenti a singole Ad Hoc Network possono colloquiare con un Distributed System attraverso dei punti di accesso, gli AccessPoint (AP).

## Tipologie di Reti Mobili

1. **Access mobility** – Sono i sistemi tipicamente indoor con raggio di azione inferiore ai 500 m, come i sistemi cordless telefonici che tramite un access point connettono alla rete fissa di tele comunicazione.
2. **Terminal mobility** – Sono i sistemi nei quali il terminale è in movimento e può accedere, rimanere connesso e identificato in una rete di telecomunicazione.
3. **Service profile portability** – In questo sistema un terminale può connettersi non solo alla propria rete ma anche ad altre reti di telecomunicazione per poter usufruire dei servizi associati al proprio profilo; esiste quindi la portabilità del proprio profilo su provider diversi, in modo trasparente per l'utente.
4. **Personal mobility** – In questo sistema è l'utente che può accedere ai servizi di telecomunicazione tramite qualsiasi terminale: la rete riconosce l'utente e non il terminale; questo permette un'offerta completa di servizi ed in questo caso si parla di Personal Communications Services (PCS).

## Autenticazione nelle reti wireless

L'autenticazione nelle reti wireless avviene solitamente attraverso il protocollo di sicurezza Wi-Fi Protected Access (WPA) o Wi-Fi Protected Access II (WPA2), che utilizzano l'algoritmo di crittografia Advanced Encryption Standard (AES) per proteggere la comunicazione tra il dispositivo e il punto di accesso (access point).

Il processo di autenticazione di solito prevede l'utilizzo di una password o di una passphrase, chiamata pre-shared key (PSK), che deve essere inserita nel dispositivo che si vuole connettere alla rete. In alternativa, è possibile utilizzare un sistema di autenticazione basato su certificati, dove il dispositivo deve possedere un certificato digitale che viene verificato dal server di autenticazione.

## Le applicazioni e i sistemi distribuiti

Le applicazioni e i sistemi distribuiti sono basati sulla suddivisione del software e delle risorse su diversi nodi di una rete. Ciò permette di ottenere una maggiore scalabilità, affidabilità e flessibilità rispetto ai sistemi centralizzati.

In questo tipo di architettura, le applicazioni sono costituite da diversi componenti software, ciascuno dei quali può essere distribuito su un nodo di rete diverso. Questi componenti interagiscono tra loro attraverso un protocollo di comunicazione standard, spesso basato su HTTP o su altri protocolli di rete.

Il sistema distribuito è costituito da diversi nodi di rete, ciascuno dei quali ospita uno o più componenti dell'applicazione. Questi nodi sono collegati tra loro tramite una rete di comunicazione, solitamente basata su Internet o su una rete privata.

Uno dei principali vantaggi dei sistemi distribuiti è la scalabilità: i nodi possono essere aggiunti o rimossi a seconda delle esigenze dell'applicazione, senza dover interrompere il funzionamento dell'intero sistema. Inoltre, i sistemi distribuiti offrono un maggiore grado di affidabilità: se uno dei nodi di rete fallisce, gli altri nodi possono continuare a funzionare, garantendo così la continuità del servizio.

Tuttavia, i sistemi distribuiti presentano anche alcuni svantaggi. Ad esempio, la complessità dell'architettura può rendere più difficile la gestione del sistema e la risoluzione dei problemi. Inoltre, la sicurezza dei sistemi distribuiti può essere una sfida, in quanto i dati devono essere protetti durante la trasmissione su una rete aperta.

Per questo motivo, l'autenticazione e l'autorizzazione sono elementi cruciali nella progettazione di sistemi distribuiti. Gli utenti devono essere autenticati prima di poter accedere alle risorse del sistema e l'autorizzazione deve essere implementata in modo tale che gli utenti possano accedere solo alle risorse a cui hanno diritto.

**SISTEMA DISTRIBUITO:** è costituito da un insieme di applicazioni logicamente indipendenti che collaborano per il perseguimento di obiettivi comuni attraverso un'infrastruttura di comunicazione hardware / software

**COMPOSTO da 3 ELEMENTI:**

- **CLIENT:** utilizzatore e richiedente.
- **SERVER:** fornitore del servizio.
- **ACTOR:** sia il client che il server.

**FAMIGLIE dei SISTEMI DISTRIBUITI:**

- Sistemi di **CALCOLO** distribuiti: calcolo ad alte prestazioni.
- Sistemi **INFORMATIVI** distribuiti: applicazioni e sistemi web.
- Sistemi distribuiti **PERVASIVI**: connessione wireless, sottoparti di sistemi più grandi (PAN, reti di sensori, sistemi domestici).

## BENEFICI della DISTRIBUZIONE:

- **Affidabilità**: indica la capacità di un sistema distribuito di funzionare in modo continuo e senza interruzioni, anche in presenza di guasti di uno o più nodi del sistema.
- **Trasparenza**: si riferisce alla capacità di un sistema distribuito di nascondere la complessità della sua architettura e di presentare un'interfaccia uniforme e coerente agli utenti e alle applicazioni.
- **Di accesso**: permette di accedere a risorse locali da remoto.
- **Di locazione**: si riferisce alla capacità di nascondere l'indirizzo IP e la posizione fisica dei nodi del sistema distribuito, rendendo più facile la gestione e la distribuzione delle risorse.
- **Di concorrenza**: indica la capacità di elaborare più richieste contemporaneamente in modo efficiente e affidabile. La concorrenza può migliorare le prestazioni e la scalabilità del sistema distribuito.
- **Di replicazione**: indica la possibilità di creare copie di dati o di componenti del sistema distribuito in modo da garantire la disponibilità delle risorse anche in caso di guasti o di congestioni.
- **Di scalabilità**: indica la capacità di un sistema distribuito di gestire un aumento del carico di lavoro in modo efficiente, senza perdere prestazioni o affidabilità.
- **Di prestazioni**: indica la capacità di un sistema distribuito di elaborare le richieste degli utenti in modo rapido e efficiente, migliorando l'esperienza dell'utente.
- **Di miglioramento**: indica la capacità di un sistema distribuito di migliorare le prestazioni, l'affidabilità e la scalabilità nel tempo, attraverso l'aggiunta di nuovi nodi o componenti. Ciò garantisce che il sistema possa adattarsi alle esigenze in evoluzione degli utenti e delle applicazioni.

## Architetture dei sistemi web

Le architetture dei sistemi web definiscono il modo in cui un'applicazione web è organizzata e si connette con altri sistemi. Le architetture più comuni sono:

1. Architettura **client-server**: in questa architettura, il client (solitamente un browser web) richiede le risorse da un server web, che le fornisce in risposta. Il client elabora quindi i dati e presenta l'interfaccia utente.

2. Architettura a **tre strati**: in questa architettura, l'applicazione è suddivisa in tre componenti: la presentazione (interfaccia utente), la logica di business (che esegue le operazioni dell'applicazione) e il database (dove vengono memorizzati i dati). Questi componenti possono essere eseguiti su diversi server.
3. Architettura a **microservizi**: in questa architettura, l'applicazione è suddivisa in servizi autonomi che possono essere distribuiti su più server. Questi servizi comunicano tra di loro utilizzando API (interfacce di programmazione delle applicazioni) e si occupano ciascuno di una specifica funzionalità.
4. Architettura a **serverless**: in questa architettura, l'applicazione è composta da funzioni che vengono eseguite su server cloud. Le funzioni vengono attivate in risposta a eventi specifici (come richieste HTTP) e non richiedono un server dedicato.

## API

Le API, acronimo di Application Programming Interface, sono un insieme di specifiche tecniche e regole che consentono ad un software di comunicare con un altro. In sostanza sono una sorta di ponte che consente ad un'applicazione di utilizzare le funzionalità di un'altra applicazione o servizio esterno.

Le API sono spesso utilizzate per la creazione di applicazioni distribuite o per l'integrazione di sistemi diversi. Ci sono diverse tipologie di API, tra cui le API web, le API di sistema e le API di terze parti:

- **API WEB**: sono tra le più utilizzate e permettono la comunicazione tra applicazioni web tramite protocolli standard come HTTP e HTTPS. Possono essere realizzate in diverse forme, come ad esempio API REST (Representational State Transfer) o SOAP (Simple Object Access Protocol).
- **API DI SISTEMA**: sono utilizzate per accedere alle funzionalità del sistema operativo o del software. Ad esempio, le API di sistema possono essere utilizzate per accedere al filesystem o alla rete.
- **API DI TERZE PARTI**: sono fornite da aziende o enti esterni e consentono l'integrazione di funzionalità specifiche all'interno delle applicazioni. Ad esempio, le API di Facebook consentono ad una applicazione di integrare le funzionalità di Facebook, come l'autenticazione, la pubblicazione di post, etc.

## Socket



I socket sono una API di comunicazione a basso livello che consente la comunicazione tra processi o applicazioni su una rete. Essi forniscono un modo standardizzato per i processi su un computer di comunicare tra loro e di scambiarsi dati. La comunicazione tramite socket utilizza due protocolli principali: TCP e UDP.

Il concetto di socket è stato sviluppato come estensione diretta del paradigma UNIX di I/O su file, che si basa sulla sequenza di operazioni open-read-write-close:

- open: permette di accedere a un file.
- read/write: accedono ai contenuti del file.
- close: terminazione dell'utilizzo del file.

Famiglie di socket:

- Internet socket (AF\_INET):  
permette il trasferimento di dati tra processi posti su macchine remote connesse tramite una LAN o Internet.
- Unix Domain socket (AF\_UNIX):  
permette il trasferimento di dati tra processi sulla stessa macchina Unix.

Funzioni più utilizzate:

- socket/serversocket: crea un nuovo socket.
- close: termina l'utilizzo di un socket.
- bind: collega un indirizzo di rete a un socket.
- listen: aspetta messaggi in ingresso.
- accept: comincia a utilizzare una connessione in ingresso.
- connect: crea una connessione con un host remoto.
- send: trasmette dati su una connessione attiva.
- recv: riceve dati da una connessione attiva.

Tipi fondamentali di Socket:

- stream socket: Operativamente, ogni processo crea il proprio endpoint creando l'oggetto socket in Java e successivamente:
  - il server si mette in ascolto in attesa di un collegamento e quando gli arriva una richiesta la esaudisce; successivamente crea un nuovo socket dedicato alla connessione.

- il client si pone in coda sul socket del server e quando viene “accettato” dal server crea implicitamente il binding (trad.legante) con la porta locale.
- datagram socket: viene realizzata la comunicazione che permette di scambiare dati senza connessione.
- raw socket: utilizzati nello sviluppo di protocolli.

## La comunicazione seriale

La comunicazione seriale è un metodo di trasmissione dati che prevede l'invio dei dati bit per bit in modo sequenziale su un singolo canale di comunicazione. Questo tipo di comunicazione è utilizzato per collegare dispositivi elettronici tra loro in modo che possano scambiare informazioni.

Per effettuare una comunicazione seriale, è necessario utilizzare un protocollo di comunicazione che definisce il modo in cui i dati vengono inviati e ricevuti. I due protocolli di comunicazione seriale più comuni sono RS-232 e RS-485.

Il protocollo RS-232 prevede la trasmissione seriale di dati in modalità asincrona, ovvero i dati vengono trasmessi senza utilizzare un clock comune per sincronizzare la trasmissione e la ricezione dei dati. Questo tipo di protocollo prevede due fili per la trasmissione dei dati (TX) e la ricezione dei dati (RX).

Il protocollo RS-485 prevede invece la trasmissione seriale di dati in modalità sincrona, ovvero i dati vengono trasmessi utilizzando un clock comune per sincronizzare la trasmissione e la ricezione dei dati. Questo tipo di protocollo prevede un solo filo per la trasmissione dei dati (TX) e un altro filo per la ricezione dei dati (RX).

## Posta elettronica

La posta elettronica (o email) utilizza diversi protocolli per il suo funzionamento. Ecco una spiegazione dei principali protocolli che vengono utilizzati:

1. **SMTP** (Simple Mail Transfer Protocol): È il protocollo di base utilizzato per inviare email da un client email (come Outlook, Gmail, Thunderbird) a un server di posta. SMTP definisce le regole per l'inoltro dei messaggi tra i server di posta elettronica.
2. **POP** (Post Office Protocol): POP permette ai client email di recuperare le email dal server di posta. Con il protocollo POP, i messaggi vengono scaricati dal

server sul dispositivo del destinatario e vengono generalmente eliminati dal server, se non specificato altrimenti.

3. **IMAP** (Internet Message Access Protocol): IMAP è un protocollo simile a POP, ma con alcune differenze importanti. Con IMAP, i messaggi email rimangono memorizzati sul server di posta anche dopo essere stati scaricati sul dispositivo del destinatario. Ciò permette di accedere alle email da più dispositivi e mantenerle sincronizzate.
4. **MIME** (Multipurpose Internet Mail Extensions): MIME è un protocollo che estende il formato dei messaggi email per consentire l'inclusione di contenuti multimediali come immagini, audio e video. MIME consente anche l'inclusione di allegati nei messaggi email.
5. **SSL/TLS** (Secure Sockets Layer/Transport Layer Security): SSL e TLS sono protocolli di crittografia utilizzati per proteggere la comunicazione tra i client email e i server di posta. SSL e TLS assicurano che le email inviate e ricevute siano crittografate e che solo il mittente e il destinatario legittimi possano accedere al contenuto.

## Porte delle applicazioni

Le **porte** assegnate alle applicazioni variano da un range di numeri predefinito. Nel contesto del TCP e UDP, ci sono due range principali per le porte:

1. **Porte ben conosciute:** Le porte ben conosciute vanno dal numero 0 al numero 1023. Queste porte sono assegnate a servizi comuni e ben noti, come HTTP (porta 80), FTP (porta 21), SSH (porta 22), HTTPS (porta 443), ecc. Di solito, queste porte sono riservate per i servizi standard e le applicazioni di sistema.
2. **Porte registrate:** Le porte registrate vanno dal numero 1024 al numero 49151. Queste porte sono assegnate da IANA (Internet Assigned Numbers Authority) per applicazioni specifiche o protocolli meno noti. Sono riservate per le applicazioni registrate presso l'IANA e possono essere utilizzate da applicazioni personalizzate o specializzate.
3. **Porte libere:** Le porte dinamiche o private vanno dal numero 49152 al numero 65535. Queste porte sono disponibili per l'assegnazione dinamica da parte dei sistemi operativi per le connessioni di rete effimere o temporanee. Sono comunemente utilizzate per le connessioni in uscita dei client.

# Sintassi di una richiesta HTTP

Una richiesta HTTP (Hypertext Transfer Protocol) è una comunicazione tra un client e un server web. La sintassi di base di una richiesta HTTP è la seguente:

```
METODO URL VERSIONE_HTTP
Header1: valore1
Header2: valore2

Corpo del messaggio
```

Dove:

- **METODO:** Specifica l'azione che il client desidera eseguire sul server, come GET, POST, PUT, DELETE, ecc.
- **URL:** L'URL (Uniform Resource Locator) che identifica la risorsa a cui si desidera accedere o su cui si desidera eseguire l'azione.
- **VERSIONE\_HTTP:** La versione del protocollo HTTP utilizzata nella richiesta.
- **Header:** Opzionale. Fornisce informazioni aggiuntive sulla richiesta, come l'User-Agent, Content-Type, ecc.
- **Corpo del messaggio:** Opzionale. Contiene dati aggiuntivi associati alla richiesta, ad esempio quando si invia un form HTML o si carica un file.

Ecco un esempio di una semplice richiesta HTTP GET:

```
GET /pagina.html HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.93 Safari/537.36
```

## Multiplexing

Il multiplexing è una tecnica utilizzata per consentire la condivisione efficiente di una risorsa tra più utenti o processi. Nel contesto delle reti di computer, il multiplexing si riferisce alla tecnica di combinare più flussi di dati in un unico canale di comunicazione, consentendo così di trasmettere più informazioni contemporaneamente.

Ci sono diversi tipi di multiplexing utilizzati nelle reti, tra cui:

1. **Time Division Multiplexing (TDM):** In TDM, il tempo viene suddiviso in intervalli di tempo più piccoli e ogni intervallo viene assegnato a un flusso di dati diverso. È come se ogni flusso di dati avesse il proprio "slot" temporale nel canale di comunicazione.
2. **Frequency Division Multiplexing (FDM):** In FDM, la larghezza di banda disponibile viene suddivisa in diverse bande di frequenza e ogni banda viene assegnata a un flusso di dati diverso. I flussi di dati utilizzano frequenze diverse per evitare interferenze.
3. **Code Division Multiplexing (CDM):** In CDM, i flussi di dati sono separati utilizzando codici unici, consentendo loro di condividere la stessa banda di frequenza contemporaneamente. Questo viene spesso utilizzato nelle reti cellulari.
4. **Wavelength Division Multiplexing (WDM):** In WDM, i flussi di dati sono separati utilizzando diverse lunghezze d'onda della luce. Ciò consente di trasmettere più flussi di dati simultaneamente su una fibra ottica.

Ogni forma di multiplexing ha le sue applicazioni specifiche e viene utilizzata per massimizzare l'utilizzo delle risorse di comunicazione in diversi contesti.